526,206

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 March 2004 (18.03.2004)

PCT

(10) International Publication Number
WO 2004/023832 A1

(51) International Patent Classification[7]: H04Q 7/32, H04L 9/32, G07F 7/10

(21) International Application Number: PCT/IB2003/003577

(22) International Filing Date: 28 August 2003 (28.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02292180.3 4 September 2002 (04.09.2002) EP

(71) Applicant *(for all designated States except US)*: **SCHLUMBERGER SYSTEMES** [FR/FR]; 50, avenue Jean-Jaurès, F-92120 Montrouge (FR).

(71) Applicant *(for MC only)*: **SCHLUMBERGER MALCO** [US/US]; 9800 Reistertown road, Owings Millq, MD 21117 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MAHALAL, Ilan** [FR/FR]; 16, avenue de Bouvines, F-75011 Paris (FR).

(74) Common Representative: **SCHLUMBERGER SYSTEMES**; C/O GUILLERM, Patrice, 50, avenue Jean-Jaurès, F-92120 Montrouge (FR).

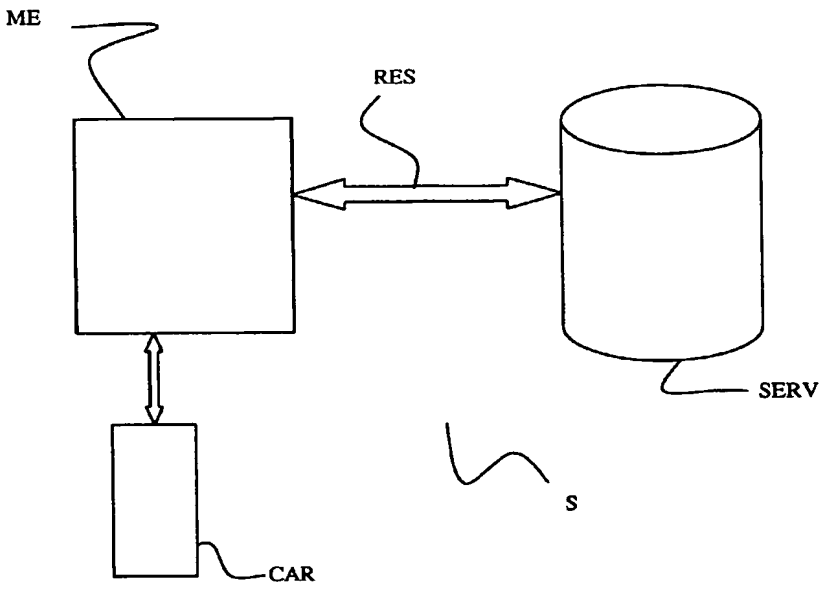
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

[Continued on next page]

(54) Title: METHOD FOR CALCULATING HASHING OF A MESSAGE IN A DEVICE COMMUNICATING WITH A SMART CARD



(57) Abstract: The invention is a method for calculating hashing of a message in a device communicating with a smart card, said device and said smart card storing the same hash function, the message comprising data blocks including secret data and other data, secret data being only known by the smart card, characterized in that the calculation of the hash of the secret data is performed in the smart card and the calculation of the hash of all or part of the other data is performed in the device, and in that, the intermediate result is transmitted from the device to the card, or inversely, depending on whether the hash calculation of the hash of a data has to be performed by the smart card or the device.

WO 2004/023832 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method for calculating hashing of a message in a device communicating with a smart card

Field of the Invention

The invention concerns a method for calculating hashing of a message in a smart card. In the following text, a smart card will designate all tamper- resistant devices able to store secret data.

The example that will be used for illustrating the invention is that of a WIM (WAP Identity Module) module coupled to a mobile phone. This smart card could also be a SIM (Subscriber Identity Module) smart card, or all other module able to store secret data and to perform Hash functions.

Prior Art

The Wireless Application Protocol (WAP) defines an industry-wide specification for developing applications that operate over wireless communication networks. The scope for the WAP Forum is to define a set of specifications to be used by service applications. The wireless market is growing very quickly, and reaching new customers and services. To enable operators and manufacturers to meet the challenges in advanced services, differentiation and fast/flexible service creation WAP Forum defines a set of protocols in transport, security, transaction, session and application layers.

The Security layer protocols in the WAP architecture can be the Wireless Transport Layer Security (WTLS) or the standard Transport Layer Security (TLS) Internet protocol. WTLS provides functionality similar to TLS but is more adapted to lower bandwidth communication channels. TLS and WTLS layer operate above the transport protocol layer. They provide the upper-level layer of WAP with a secure transport service interface and also provide an interface for managing (eg, creating and terminating) secure connections. The primary goal of the WTLS or TLS layers is to provide privacy, data integrity and authentication between two communicating applications.

For optimum security, some parts of the security functionality need to be performed by a tamper-resistant device, so that an attacker cannot retrieve sensitive data. Such data is especially the permanent private keys used in the WTLS or TLS handshakes with client authentication, and for making application level electronic signatures (such as confirming an application level transaction).

In particular, when a message has to be hashed in a mobile coupled to a WIM module, all the blocks are transferred from the mobile to the WIM for being hashed. Then, the WIM sends the result to the mobile. An example of a WIM implementation is the smart card CAR. In the phone, it can be the Subscriber Identity Module SIM card or an external smart card. The problem is that, in the WIM, resources are very limited; consequently, calculations take a lot of time.

For example, in WTLS and TLS, the Mobile Equipment sends to the server a message called "Finished" message, which is always sent to the server at the end of a handshake to verify that the key exchange and authentication processes were successful between the mobile and the server. The Mobile Equipment uses the smart card for calculating the data to send in the "Finished" message and also the data that should be received from the server. In order to do that, the mobile ME issues the "Client Finished Check" and "Server Finished Check" commands to the smart card CAR. Using a Pseudo Random Function (PRF), the smart card calculates a requested number of bytes based on the session master secret, and a seed value received from the mobile. The card then returns the bytes to be used by the mobile in the "Finished" message. For calculating the Client Finished Check data, the mobile uses a primitive called WIM-PHash primitive with the following input data parameter:

"client finished" + Hash(handshake_messages)

The "Hash(handshake_messages)" is defined as the SHA-1 and/or MD5 hash (depending on protocol) of the concatenation of all previous handshake messages that were exchanged up to but not including the

"Finished" message. The primitive then returns to the mobile the needed data block.

We will refer the standard for more details about the commands and primitives which are cited above.

In the same manner, for Calculating the server finished check, the mobile ME uses the WIM-PHash primitive with the following input data parameter:

"server finished" + Hash(handshake_messages).

The primitive then returns to the mobile the needed data block.

In SSL, the parameters that are sent to the WIM for the "Finished" message are different. When we perform the finished check in SSL, it is necessary to perform a hash on:

'handshake_messages + Sender + master_secret + pad1'. Comparing with WTLS and TLS, we see that the Hash should be calculated also over the session "master secret" in addition to "handshake_messages". This poses a problem since the mobile ME does not know the value of the master secret as it is securely stored in the smart card CAR and is never exposed externally. Consequently, the following data: **'handshake_messages + Sender + master_secret + pad1'** has to be sent to the WIM for being hashed. Nevertheless, resources are very limited in the WIM, consequently calculations in the smart card take a lot of time.

Invention

The aim of the invention is to hash a message in an efficient manner reducing the consumption of resources in the WIM.

The invention is a method for calculating hashing of a message in a device communicating with a smart card, said device and said smart card storing the same hash function, the message comprising data blocks including secret data and other data, secret data being only known by the

smart card. According to the invention, the calculation of the hash of the secret data is performed in the smart card and the calculation of the hash of all or part of the other data is performed in the device.

We will that, the intermediate result is transmitted from the device to the card, or inversely, depending on whether the hash calculation of the hash of a data has to be performed by the smart card or the device.

In this way, the invention avoids time consuming to calculate a Hash function in the smart card since the device, in particular a mobile phone, can usually do it faster as it has a stronger processor.

It will be easier to understand the invention on reading the description below, given as an example and referring to the attached drawings.

In the drawings:

Figure 1 represents an example of a data processing system S in which the invention may be applied.

Figures 2-4 are views of different types of messages including secret data.

Detailed Description of Examples Illustrating the Invention

In order to simplify the description, the same elements illustrated in the drawings have the same references.

Figure 1 represents a system S. In our example, this system includes a smart card CAR coupled to a mobile phone ME communicating with a server SERV through a network RES.

Generally, the smart card is used to store and process information needed for user identification and authentication. The smart card CAR

stores the client sensitive data, especially keys and sessions master secrets.

The smart card cn be a WIM module. The WIM (WAP Identity Module) is a security token standardized in the WAP Forum. We will refer to this standard for more details on the module WIM. As mentioned above, the WAP Forum WIM specification describes how the WIM is used with TLS and WTLS and in application level services.

Generally, as mentioned above, when a message includes keys and master secrets and that this one has to be hashed in a mobile coupled to a WIM module, all the blocks are transferred from the mobile to the WIM for performing a Hash step. Then, the WIM sends the result to the mobile. All operations where keys and master secrets are involved are performed internally in the module WIM.

Generally, a Hash function works on a fixed length of data input and the result is carried on to the next iteration. It calculates a hash on the first block of the data (64 bytes for SHA-1), then carry the result to the calculation of the Hash on the second block and continue like that until all input data is consumed.

In our example we want to hash a data input, called message MF in the following description, including:

"PD + SD"

where the "+" operator means concatenation.

This data message MF comprises data blocks including

- secret data SD, which could be the " master secret" data
- and other data PD, which could be the "handshake_messages"

According to the invention, the mobile ME can start calculating the hash over the other data PD which are public. The result of this calculation constitutes an intermediate result R. Then, The mobile ME sends the

intermediate result R and the remaining secret data SD to the smart card CAR. The smart card continues the hash calculation internally by using the intermediate result R, the remaining secret data SD and the additional data (e.g. "master_secret") that is kept internally in the smart card CAR. Once the calculation is finished, the smart card send the corresponding result to the mobile ME.

So, Generally, according to the invention, if a secret data SD is followed by the other data PD in the message MF (see figure 4), the smart card starts calculating the hash of all blocks that include a secret data SD and then sends the corresponding intermediate result R to the ME that continues the hash calculation by using the intermediate result R and the remaining data PD. For example, the data SDC including secret data is hashed in the smartcard. On the contrary, if data PD is followed by the other data SD (see figure 3), the mobile ME starts calculating the hash of the data PD and then send the corresponding intermediate result R and remaining part RP of last hash block to the smart card that continues to do the hash calculation internally by using the intermediate result R, last hash block and the remaining data SD.

Advantageously, if a block includes a part comprising secret data SD and another part comprising other data PD, the smart card calculates the hash of this block. In this way, the transfer of data is decreased between the mobile ME and the smart card CAR.

This invention also formalizes the way by which the intermediate results R are sent to the smart card in order to use the same convention of command exchanged between the mobile ME and the smart card CAR for other primitives. In our example, the mobile ME will send the hashed intermediate result R and other data if needed with the "WIM MSE-Set" command. These parameters will be put in a newly defined "SSL security environment" in the smart card CAR. In our example, The SSL security environment will implement acceptance of these parameters via the "MSE-

set" command, which should be called before invoking the "PSO" command for calculating the "Finished" message.

In our example, the device is implementing the Transport Layer Security protocol SSL (Secure Socket Layer) and the smart card is a WAP Identity Module (WIM). More specifically, the message MF is called "Finished" in the SSL protocol. The secret data SD is an SSL session master secret.

The invention also concerns a communication device ME characterized in that it includes a program for performing the following steps:

- a hashing step in which all or part of said other data PD are hashed in said communication device,
- a requesting step in which, said communication system request the smart card to perform the hash of all the secret data SD.

The invention also concerns a smart card CAR characterized in that said smart card includes a program for performing, when requested by the communication device ME, a step of hashing said secret data SD.

The main advantage of the above solution is speed. It will take more time to write the whole data in a file in the WIM and then have the WIM read it and hash it. Speed is very important in the handshake and it is very important to optimise it. If it takes more than a few seconds to establish a secure session it is not very convenient for the user. The other advantage is to avoid the need to store a big block of data in the WIM for a specific primitive. This invention defines a solution for calculating the "Finished" message by the WIM module for SSL in an efficient manner and without the need to send the whole "handshake_messages" data block to store in the WIM. For example, In WTLS, protecting secure sessions are relatively long living – which could be several days. The invention will avoid frequent

full handshakes which are relatively heavy both computationally and due to large data transfer.

Of course, the invention is not limited to SSL but can be used in other technical fields.

Claims:

1. A method for calculating hashing of a message (FM) in a device communicating with a smart card, said device and said smart card storing the same hash function, the message comprising data blocks including secret data (SD) and other data (PD), secret data (SD) being only known by the smart card, characterized in that the calculation of the hash of the secret data (SD) is performed in the smart card and the calculation of the hash of all or part of the other data (PD) is performed in the device.

2. The method according to claim 1, characterized in that, if data (SD) is followed by the other data (PD) in the message (FM), the smart card starts calculating the hash of all blocks that include a secret data (SD) and then sends the corresponding intermediate result (R) to the (ME) that continue the hash calculation by using the intermediate result (R) and the remaining data (PD).

3. The method according to claim 2, characterized in that, if said Hash function hashes a message block by block, and if a block includes a part comprising secret data (SD) and another part comprising other data (PD), the smart card calculates the hash of this block.

4. The method according to claim 1, characterized in that, if data (PD) is followed by the other data (SD), the device (ME) starts calculating the hash of (PD) and then sends the corresponding intermediate result (R) and remaining part (RP) of last hash block to the smart card that continue to do the hash calculation internally by using the intermediate result (R), last hash block and the remaining data (SD).

5. Communication device ME being able to be coupled to a smart card CAR, said device and said smart card storing the same hash

function, the message (MF) comprising data blocks including secret data (SD) and other data (PD), secret data (SD) being only known by the smart card, characterized in that said device includes a program for performing the following steps:

- a hashing step in which all or part of said other data (PD) are hashed in said communication device,
- a requesting step in which, said communication system request the smart card to perform the hash of all the secret data (SD).

6. A smart card (CAR) coupled to a Communication device (ME), said device and said smart card storing the same hash function, the message (MF) comprising data blocks including secret data (SD) and other data (PD), secret data (SD) being only known by the smart card, characterized in that said smart card includes a program for performing, when requested by the communication device (ME) as defined in claim 5, a step of hashing of all of said secret data (SD).

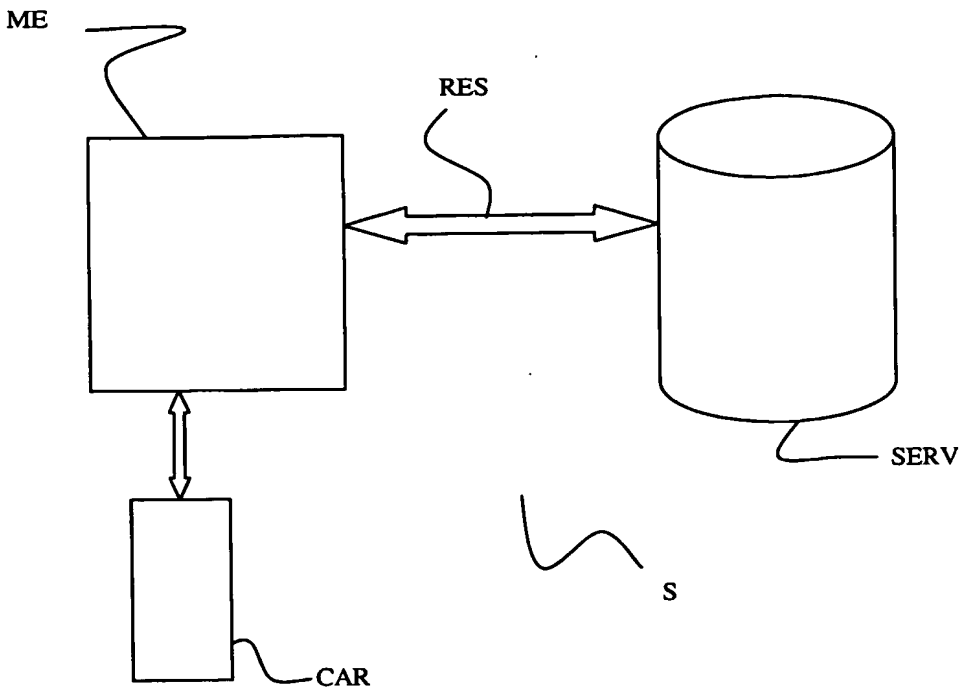


Figure 1

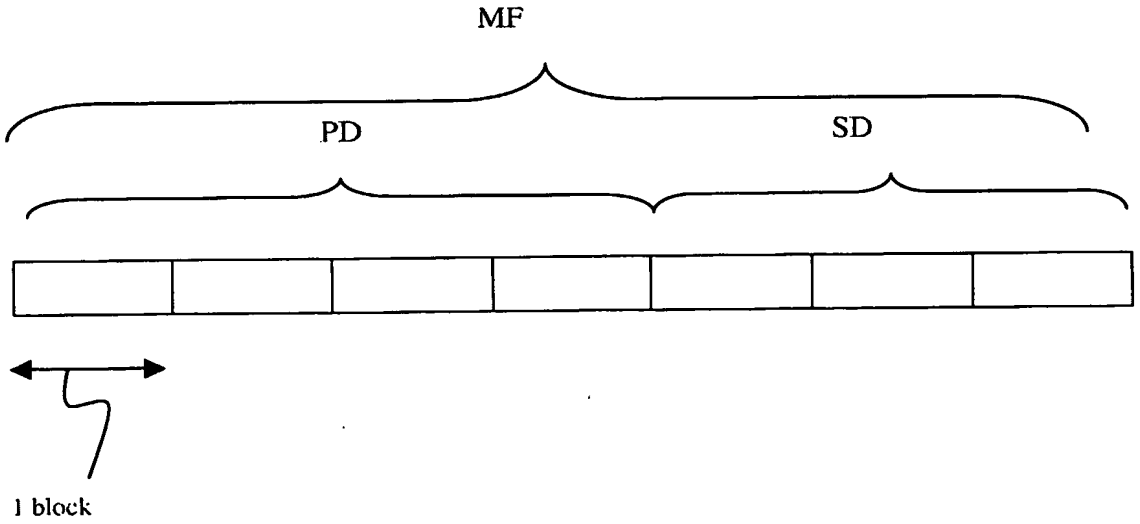


Figure 2

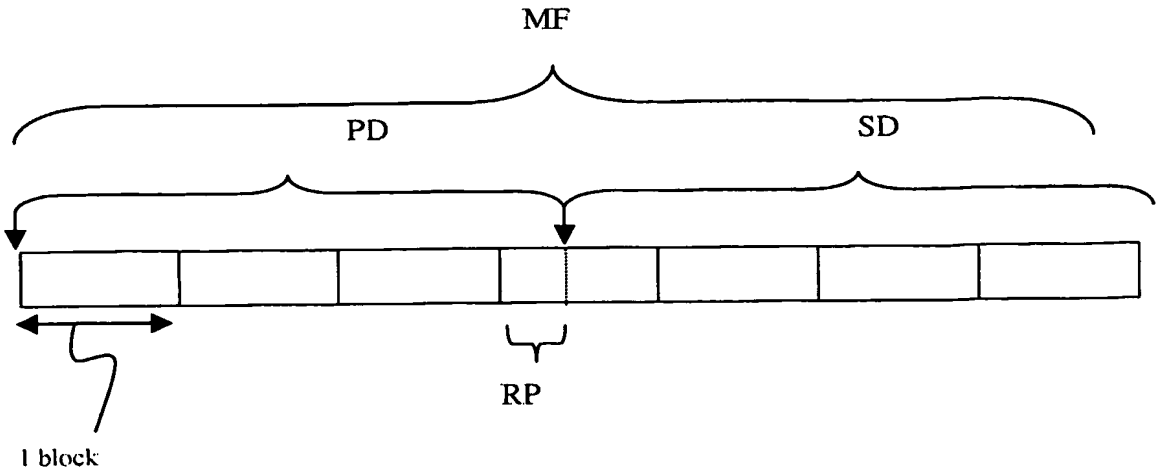


Figure 3

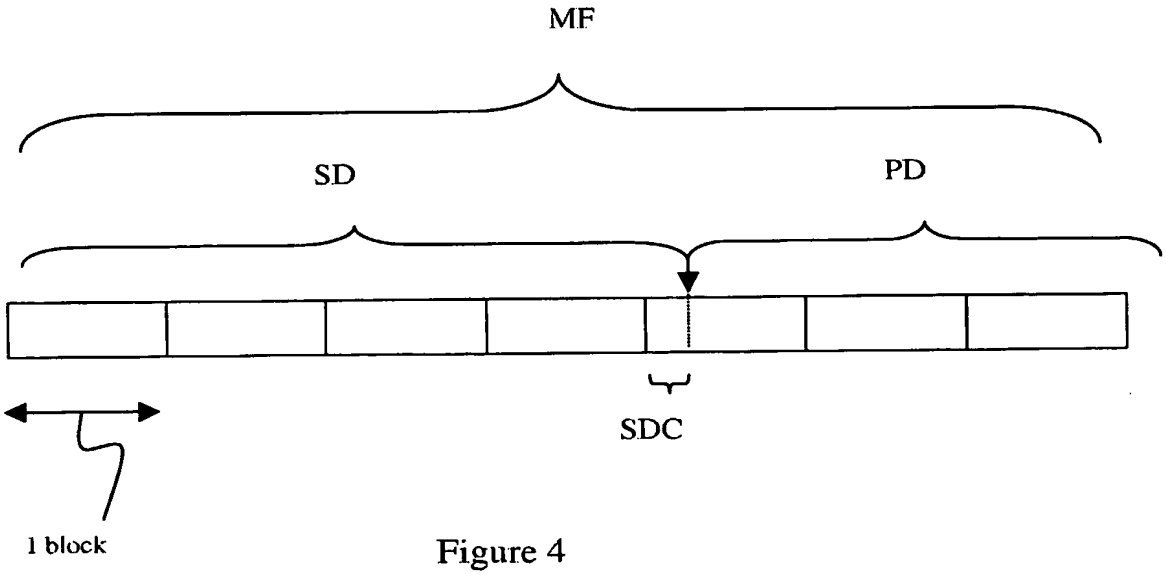


Figure 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB 03[illegible]577

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/32 H04L9/32 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02 054663 A (QUALCOMM INC) 11 July 2002 (2002-07-11) abstract	1-4
Y	page P2, line 9,19-21 page 3, line 15 -page 5, line 10 page 10, line 14 -page 12, line 19 page 7, line 26 -page 8, line 26 figure 3	5,6

Y	FR 2 817 107 A (MERCURY TECHNOLOGIES SARL) 24 May 2002 (2002-05-24)	5,6
A	abstract page 3, line 1 -page 4, line 15 figure 1	1-4

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 November 2003	11/12/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bec, T

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	"Wireless Transport Layer Security" WAP FORUM, 'Online! 6 April 2001 (2001-04-06), pages 1-106, XP002223489 Retrieved from the Internet: <URL:http://wapforum.org> 'retrieved on 2002-11-19! page 17 page 19 page 35 page 51-53 page 72-73 page 78	1-6
A	WO 01 84761 A (LAUPER ERIC ;WIEDMER EDWIN (CH); BUTTYAN LEVENTE (CH); SWISSCOM MO) 8 November 2001 (2001-11-08) abstract page 4, line 15 - line 30 page 6, line 8 -page 8, line 25 page 10, line 1 -page 11, line 8 page 12, line 14 - line 30 page 14, line 11 -page 16, line 30 page 24, line 10 -page 27, line 27 figures 4,5,7	1-6
A	WO 01 43472 A (SONERA OYJ ;VIRKKULA PETRI (FI); HEINONEN PETTERI (FI)) 14 June 2001 (2001-06-14) abstract page 1, line 1 - line 17 page 4, line 30 -page 5, line 18 page 6, line 21 -page 7, line 2 page 7, line 35 -page 8, line 3 page 8, line 32 -page 9, line 35 page 11, line 29 -page 12, line 7 figures 1,3	1-6

INTERNAT[redacted]AL SEARCH REPORT

Internatio[redacted]tion No
PCT/IB 0[redacted]577

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 02054663	A	11-07-2002	US	2002091931 A1	11-07-2002
			EP	1348274 A2	01-10-2003
			WO	02054663 A2	11-07-2002
			US	2002091933 A1	11-07-2002
FR 2817107	A	24-05-2002	FR	2817107 A1	24-05-2002
WO 0184761	A	08-11-2001	AU	6589701 A	12-11-2001
			AU	7520300 A	12-11-2001
			WO	0184761 A1	08-11-2001
			WO	0184763 A2	08-11-2001
			EP	1277299 A1	22-01-2003
			EP	1277301 A2	22-01-2003
			US	2003041244 A1	27-02-2003
WO 0143472	A	14-06-2001	FI	992661 A	11-06-2001
			AU	2375101 A	18-06-2001
			EP	1236367 A1	04-09-2002
			WO	0143472 A1	14-06-2001